Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband	)	WC Docket No. 16-106
and Other Telecommunications Services	)	
	)	

COMMENTS OF THE ASSOCIATION OF NATIONAL ADVERTISERS

Daniel L. Jaffe
Group Executive Vice President,
Government Relations
Association of National Advertisers

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband	)	WC Docket No. 16-106
and Other Telecommunications Services	)	
	)	

I. INTRODUCTION AND SUMMARY

The Association of National Advertisers (ANA), on behalf of its members, hereby files comments in response to the Federal Communications Commission's ("FCC" or the "Commission") Notice of Proposed Rulemaking (NPRM) seeking to expand the Consumer Proprietary Network Information (CPNI) rules to broadband Internet access service ("BIAS").[1] Founded in 1910, ANA's membership includes more than 700 companies with 10,000 brands that collectively spend over $250 billion in marketing and advertising. ANA provides leadership for small businesses and household brands that advances marketing excellence and shapes the future of the industry. ANA includes the Business Marketing Association (BMA) and the Brand Activation Association (BAA), which operate as divisions of the ANA, and the Advertising Educational Foundation, which is an ANA subsidiary. The ANA is also a founding member of the Digital Advertising Alliance (DAA) Self-Regulatory Program. The DAA establishes and enforces responsible privacy practices across the industry for relevant digital advertising,

[1] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Dkt. No. 16-106 (Apr. 1, 2016) ("NPRM").

providing customers with enhanced transparency and control.[2] ANA promotes the interests of marketers and protects the First Amendment rights and well-being of the marketing community.

The proposed rules represent a dramatic and counterproductive expansion of the FCC's jurisdiction over privacy matters. In addition, mandatory opt-in consent for most interest-based[3] online advertising facilitated by BIAS providers would dramatically curtail the effectiveness of online advertising, as evidenced by a Massachusetts Institute of Technology ("MIT") study that found that advertising effectiveness in the European Union (EU) fell by 65 percent following the implementation of the EU Privacy Directive.[4] One study, utilizing these findings, found that U.S. websites would lose $33 billion over five years if Congress mandated EU-style opt-in consent for interest-based advertising.[5] Traditional website publishers and bloggers, many of whom are already moving behind paywalls or facing continued threats from ad blocking, would be further undermined by these proposals.[6]

BIAS providers are major advertisers that could be significantly disadvantaged in the interest-based advertising market by the FCC's proposal, resulting in widespread content and revenue loss and less effective and relevant advertising to the public. These rules, however, hurt

---

[2] *See* Digital Advertising Alliance, *Digital Advertising Alliance (DAA) Self-Regulatory Program*, www.aboutads.info (for more information regarding the DAA Program and its multifaceted Privacy Principles).

[3] Interest-based advertising, also known as relevant advertising and online behavioral advertising, uses information gathered about users' visits over time and across different websites or applications in order to help predict preferences and show ads that are more likely to be of interest to users. *See* Digital Advertising Initiative, *About Interest-Based Advertising* (Feb. 24, 2015), www.aboutads.info/how-interest-based-ads-work#aboutinterest.

[4] Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, MIT Open Access Articles 2 (2010), https://dspace.mit.edu/openaccess-disseminate/1721.1/64920.

[5] *See* NetChoice, https://netchoice.org/library/estimate-of-us-revenue-loss-if-congress-mandated-opt-in-for-interest-based-ads.

[6] *See, e.g.*, The New York Times, www.nytimes.com; The Washington Post, www.washingtonpost.com; *see also* NetChoice, https://netchoice.org/library/estimate-of-us-revenue-loss-if-congress-mandated-opt-in-for-interest-based-ads.

a far broader range of advertisers. As detailed in this filing, this extraordinarily restrictive opt-in privacy regime will inevitably diminish access to vast amounts of non-sensitive information that provides all segments of the advertising community the ability to develop ads relevant to consumer interests, generating enormous U.S. economic activity.

The proposed opt-in approval rule is also completely unnecessary and counterproductive because the current system is working well and fostering the public interest. Broad, effective self-regulation, buttressed by Federal Trade Commission (FTC) and state enforcement, provides strong protections to consumers and appropriate business interests. The existing sound regulatory structure should not be replaced with the NPRM's hastily developed and ill-considered proposed rules. The Open Internet Order, which the FCC cites as the basis of its authority to regulate broadband privacy,[7] is still under careful court review and the FCC is on uncertain footing for the broad and sweeping changes it proposes.[8]

Even if the Open Internet Order is upheld, the NPRM would still be highly misguided and unjustified. The proposed rules will have serious adverse effects, including:

- Fostering an online ecosystem that would be less protective for consumers and that would cause them to be barraged with intrusive, annoying privacy popups online (and even worse, over their mobile phones).
- Creating the potential to accelerate further movement of content behind paywalls.
- Increasing the potential for BIAS providers to raise subscription rates due to lost advertising revenue.
- Furthering the potential for negative effects on downstream advertisers that rely on information from BIAS providers to provide interest-based advertising.

[7] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, 30 FCC Rcd 5601 (2015).

[8] *See* Joint Brief for Petitioners US Telecom, NCTA, CTIA, ACA, WISPA, AT&T, and CenturyLink, *U.S. Telecom Ass'n. v. FCC*, No. 15-1063 (D.C. Cir. Jul. 30, 2015).

- Upending over a decade of privacy precedent carefully developed by the FTC, state governments, and self-regulatory organizations that distinguishes the treatment of sensitive and non-sensitive personally identifiable information, resulting in substantial consumer confusion in the Internet and mobile marketplace.

Consumers have demonstrated that they prefer interest-based advertising over ads unrelated to their interests.[9] Interest-based advertisements respect consumers' precious time in a fast-paced environment. ANA does not believe that the Commission has analyzed sufficiently potential consumer behavior and the NPRM's potentially severe negative impacts on consumers, BIAS providers, other impacted advertisers, the Internet ecosystem and the U.S. economy.[10] These significant negative impacts make clear that the NPRM does not further the public interest and therefore should not be adopted.

II. ADVERTISING BENEFITS BOTH CONSUMERS AND THE ECONOMY

Advertising provides enormous beneficial content and information to consumers in the digital marketplace. It is a powerful engine for economic growth and development, providing employment opportunities and job diversity, improving consumers' standard of living by facilitating informed decision-making, ensuring the survival of all media availing themselves of the Internet, creating healthy competition among products, and otherwise benefiting the economic development of the nation. An important recent study by the highly-regarded IHS Economics and Country Risk group analyzed advertising's economic contributions in the U.S. on a national, state and regional basis. The study found that in 2014, an estimated $297 billion was spent on

[9] Katy Bachman, *Poll: Targeted Advertising Is Not the Bogeyman*, Adweek (Apr. 18, 2013), www.adweek.com/news/technology/poll-targeted-advertising-not-bogeyman-updated-148649.

[10] ANA also notes that a recent Working Paper published by the Institute for Information Security & Privacy at Georgia Tech raises questions regarding BIAS providers' visibility into consumers' browsing activities and merits further investigation by the Commission. *See* Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Inst. for Info. Security & Privacy at Georgia Tech 3 (Feb. 29, 2016), www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

advertising; advertising accounted for 16 percent of the $36.7 trillion in total U.S. sales; every dollar of advertising contributed $19 in sales; and advertising spending created $2.4 trillion in direct consumer sales. Advertising contributed $3.4 trillion (19%) to the U.S. GDP, supported 20 million U.S. workers, and overall supported $1.9 trillion in salaries and wages in 2014.[11]

In addition, a recent report indicates the critical role that advertising plays in the digital economy. On February 3, 2016, the Direct Marketing Association (DMA) issued a report finding that the data-driven marketing economy contributed nearly one million jobs in 2014 and added $202 billion in revenue to the U.S. economy.[12]

As discussed above, digital advertising, a substantial part of which includes relevant advertising, is indeed a growth powerhouse that supports much of the freely-available content online. Half of the data-driven marketing economy relies on the exchange of information, and restricting the exchange of consumer data would impact $100 billion in revenue to the U.S. economy and over 500,000 American jobs.[13] An April 21, 2016 report from the Interactive Advertising Bureau (IAB) showed that U.S. digital advertising revenues alone reached an all-time high of $59.6 billion in 2015. This marks a 20 percent increase over the record-breaking revenues of 2014 and the sixth year in a row of double-digit growth for the industry.[14]

---

[11] Leslie Levesque, Bob Flanagan & Mark Lauritano, *Economic Impact of Advertising in the United States*, IHS Economics and Country Risk (2015), www.ana.net/getfile/23045.

[12] Direct Marketing Association, (Dec. 2015), http://thedma.org/advocacy/data-driven-marketing-institute/value-of-data.

[13] *Id.*

[14] Interactive Advertising Bureau, *IAB Internet Advertising Revenue Report Conducted by PricewaterhouseCoopers (PWC)* (Apr. 21, 2016), www.iab.com/internetadrevenue.

These facts are not lost on consumers, as demonstrated by a Zogby study commissioned by the DAA and updated this past April.[15] Consumers were asked the following question: "Which of the following would you prefer: an Internet where there are no ads, but you have to pay for most content you read/see like blogs, entertainment sites, video content and social media, or today's Internet in which there are ads, but most content is free?" Over 85 percent of the consumers surveyed prefer an advertising-supported Internet where most of the content is free.[16]

These studies are instructive, and the Commission needs to allow more time than it has provided for other stakeholders to sufficiently study the impact that the proposed rules will have on this thriving advertising economy, including the economic impacts on businesses, advertising, consumers, and the general Internet and mobile marketplace. Failure to carry out this careful analysis will make it impossible to draw reasoned conclusions on the proposed privacy NPRM's furtherance of the public interest.

Some Commissioners also recognize the importance of advertising to the economy and content delivery. For example, Commissioner O'Rielly stated at a conference held by ANA last year, "(W)ithout advertising and the benefits it brings, the cost of every product and service in America would be increased substantially. A threat to your industry also means risking significant job loss, innovation and competition in the many business sectors that are only able to survive and/or grow because of advertising revenues."[17]

---

[15] Zogby Analytics, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet: Summary Report* (May 2016), www.aboutads.info/sites/default/files/resource/ZogbyAnalyticsConsumerValueStudy2016.pdf.

[16] *Id.*

[17] Michael O'Rielly, Commissioner, FCC, Remarks before the Association of National Advertisers 1 (Apr. 1, 2015), www.fcc.gov/document/commissioner-oriellys-remarks-ana.

III. THE COMMISSION'S RATIONALE FOR IMPOSING SWEEPING CONSUMER OPT-IN REQUIREMENTS IS NOT JUSTIFIED AND IGNORES MODERN MARKETPLACE AND TECHNOLOGICAL REALITIES

The Commission alleges that its sweeping opt-in consent proposal is justified to "materially advance" an interest in "protecting the privacy of customer information."[18] Such protection is necessary, according to the Commission, because "the vast majority of adults deem it important to control who can get information about them." The Commission further argues that "increasing the number of entities that have access to customer personal information ("PI") logically increases the risk of unauthorized disclosure by both insiders and computer intrusion… third-party entities receiving customer information have no direct business relationship with the consumer and, hence, a reduced or absent incentive to honor the privacy expectations of those customers."[19] The Commission, however, offers insufficient evidence that these concerns are legitimate or that they will result in tangible harm to consumers. Moreover, even assuming that any of these concerns are legitimate or harmful, the Commission offers totally insufficient explanation as to why an opt-in approval framework would remediate them.

Consumers' views on information control. While some consumers may express a general desire to control information about themselves, the Commission itself notes that a 2016 Pew study found that consumers are more concerned about "annoying" follow-up e-mails and potentially abusive uses of data than about data collection and sharing itself.[20] The Commission does not provide any evidence to demonstrate that such interest-based advertising could result in tangible

[18] NPRM ¶ 129.

[19] NPRM ¶129.

[20] NPRM ¶129 n.226 (citing Lee Raine & Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center 5, 6 (Jan. 14, 2016) ("2016 Pew Study")).

harm to consumers. Furthermore, any consumers that are uncomfortable with such advertising may also elect to opt out under the current DAA framework, obviating the need for an opt-in regime.[21]

Unauthorized disclosures. The Commission cites no evidence that the non-sensitive customer information collected or shared by BIAS providers is particularly prone to unauthorized disclosure. Hackers and insiders are more likely to target sensitive information that can be sold for high profits, such as payment card information and health records.[22] The T-Mobile breach cited by the Commission, for example, involved Social Security numbers.[23] Even if wrongdoers targeted non-sensitive information (such as consumers' shopping preferences), disclosures of such information are unlikely to cause consumers actual harm.

Lack of incentive to honor privacy expectations. The Commission's assertion that third parties that receive customer personal information (PI) from BIAS providers have reduced incentive to protect customer privacy is unfounded. Edge providers (the typical recipients of information shared by BIAS providers) are subject to FTC enforcement, and the Commission itself notes that the FTC "actively enforces the prohibitions in its organic statute against unfair and deceptive practices against companies in the broadband ecosystem...that are engaged in practices that violate customers' privacy expectations."[24] If avoiding FTC enforcement is not incentive

---

[21] *See* Section V *infra*.

[22] *See* Kamala Harris, *California Data Breach Report* (Feb. 2016), https://oag.ca.gov/breachreport2016 (finding that "more of the most sensitive personal information – Social Security numbers and medical information – was breached than other data types"). Bear in mind that even during the Ashley Madison breach, it was sensitive data that was released, such as sexual orientation and payment contact information to learn true identity.

[23] NPRM ¶129 n.227; T-Mobile, *Frequently Asked Questions about the Experian Incident* (Oct. 8, 2015), www.t-mobile.com/landing/experian-data-breach-faq.html.

[24] NPRM ¶132.

enough, many BIAS providers also contractually obligate recipients of customer information to use such information only as directed by that provider and in a manner consistent with the provider's privacy policy.[25]

The Commission's proposal is also at odds with consumers' demonstrated preferences with respect to Internet browsing. Consumers want, expect, and benefit from interest-based advertising. In fact, without such ads, they are likely to receive ads that are totally irrelevant to them, causing annoyance and waste. A consumer searching for beach vacation deals during the winter, for example, is far more likely to benefit from interest-based ads featuring discounts on swimwear than from non-interest-based ads featuring discounts on ski equipment. According to a 2016 Adlucent study, 71% of consumers surveyed said they would prefer ads that are tailored to their personalized interests and shopping habits.[26] Within the same study, the overwhelming majority of consumers, 87%, believed personalized advertising means unique content, based on their previous purchases or shopping behavior and delivered at a time when they are looking to purchase a product.[27] As discussed below, such data is used responsibly under existing self-regulatory frameworks, strengthened by FTC and state enforcement if companies do not follow their privacy pledges, that make the NPRM's opt-in approval proposal all the more unnecessary.

IV. EXISTING SELF-REGULATORY PROGRAMS PROVIDE CONSUMER TRANSPARENCY, NOTICE AND CHOICE FOR INTEREST-BASED ADVERTISEMENTS

---

[25] *See infra* n. 69 and accompanying text.

[26] Holly Pauzer, *71% of Consumers Prefer Personalized Ads*, Adlucent (May 12, 2016), www.adlucent.com/blog/2016/71-of-consumers-prefer-personalized-ads.

[27] *Id*.

Currently, online data collection, use and sharing activities are governed by industry self-regulatory programs established by the DAA, DMA and the Network Advertising Initiative ("NAI"), and are strongly reinforced by the FTC's unfair and deceptive advertising practices jurisdiction as well as "little FTC Act" enforcement under state law. A change in the existing privacy consent framework is unnecessary, particularly given the privacy-protective attributes of these self-regulatory programs:

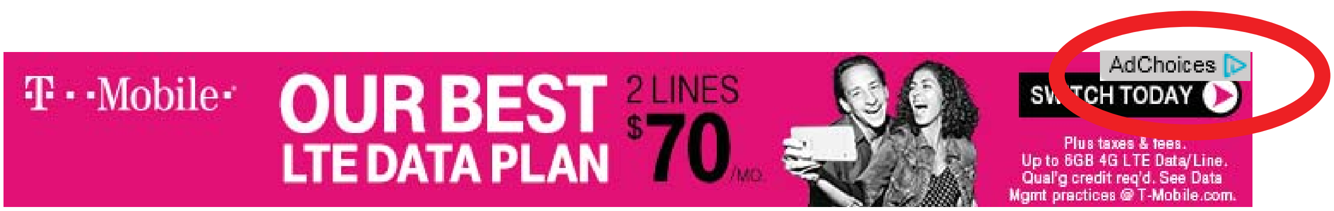
- *Robust Notice & Choice:* The DAA and NAI privacy self-regulatory programs require transparent consumer notices, real-time disclosure of data collection and effective consumer choice (consumers can opt out of virtually all cookies and beacons present on a website) for interest-based ads.
- *Opt-In Consent Requirements for Sensitive Data:* These programs also require consumer opt-in consent for sensitive data collection, storage or use, even if de-identified.[28] This means that these frameworks already require customers' opt-in consent for the most sensitive types of information, including precise location data, sexual orientation, children's data, financial information, medical prescriptions and diagnoses, and Social Security numbers or other government identifiers.
- *Self-Regulatory Enforcement:* These programs have strong, effective self-regulatory accountability mechanisms. If a company fails to meet its obligations under, for example, the DAA's independent accountability programs enforced and administered by the Council for Better Business Bureaus ("CBBB") and the DMA,

[28] *See* DAA, *Self-Regulatory Principles for Online Behavioral Advertising* 40 (July 2009), www.aboutads.info/resource/download/seven-principles-07-01-09.pdf ("DAA OBA Principles"); NAI, *2015 Update to the NAI Code of Conduct* 7, 8, www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf ("NAI Code of Conduct").

the CBBB or the DMA will notify the company of non-compliance and work to bring a company into compliance. The CBBB publicly reports its decisions and has brought 66 enforcement actions since the DAA Program went into effect.

- *Enhanced FTC Enforcement in Two Ways:* First, these programs require adherents to affirmatively pledge compliance with the standard in their privacy policies, subjecting them to enforcement under Section 5 of the Federal Trade Commission Act if they do not comply.[29] Second, should any program encounter violations that cannot be cured by the self-regulatory process, the privacy self-regulatory organizations are empowered to send cases to the FTC for review.[30]

The DAA opt-out process is very easy to use. As shown below, a consumer is alerted to an interest-based advertisement with the blue AdChoices icon (placed on the Internet trillions of times every month):



The AdChoices icon is now by far one of the most ubiquitous symbols on the Internet. When consumers click on the icon, they are typically linked to the precise place on a website publisher's privacy policy where they can find a link to the DAA's or NAI's opt-out page. Then, when a

---

[29] 15 U.S.C. § 45.

[30] *See* NAI Code of Conduct, *supra* n. 28 at 9 (providing for FTC referral in the case of non-compliance); *see also* Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *U.S. v. Google*, No. CV 12-04177 SI 2 (N.D. Cal. Nov. 16, 2012) (noting that the FTC brought an enforcement action against Google for failing to comply with its representations that it violated the NAI Code of Conduct).

consumer clicks a DAA opt-out link,[31] the following screen will appear, providing a consumer with opt-out options:

The DAA, DMA and NAI continue to update their programs to make them more consumer-friendly. Consumers may opt out of any DAA-participating cookies or beacons that customize ads for the consumer's browser on an individual company basis or may opt out of receiving interest-based advertising with the click of a single opt-out button. The programs have also expanded to mobile and cross-device interest-based advertising to reflect technological change. Further, the DAA opt-out program recently launched a DAA En Español program for Spanish speaking users in the U.S. This program is widely utilized. The DAA program has expanded to thirty-five countries worldwide; there have been more than 54 million visitors to the DAA opt-out page, and over 7 million members of the public have utilized this method to opt out of receiving interest-based advertising.

Many participating organizations spent years building these programs and established enforcement procedures to hold industry participants accountable. Large telecommunications providers helped develop the existing standards, were early supporters of the programs and are strong advocates for the programs today. The self-regulatory programs are robust, carefully

[31] A similar interface is used for the NAI opt-outs, *available at* www.networkadvertising.org/choices/#completed.

considered, and based on consumers' opt-out approval (except in the case of sensitive data collection).

This NPRM, however, would require opt-in consent from customers before sharing applicable customer information with non-communications-related affiliates.[32] Opt-in consent for most third-party uses of data would detrimentally change the entire process of consent for a whole segment of program adherents. This drastic and unwarranted change is all the more disappointing considering that only four short years ago, all DAA member organizations were applauded in a White House ceremony for their efforts in increasing consumer transparency and choice.[33] In the intervening years, the programs have only improved and garnered support from a number of FTC Commissioners.[34] There has been a vast increase in self-regulatory program adherents and robust

[32] NPRM ¶18.

[33] *See* Digital Advertising Alliance, *White House, DOC and FTC Commend DAA's Self-regulatory Program to Protect Consumer Online Privacy* (Feb. 23, 2012), www.prnewswire.com/news-releases/white-house-doc-and-ftc-commend-daas-self-regulatory-program-to-protect-consumer-online-privacy-140170013.html.

[34] *See, e.g.*, Terrell McSweeny, Commissioner, FTC, Remarks at Association of National Advertisers Advertising Law & Public Policy Conference (Mar. 31, 2015) ("I'd be remiss if I didn't commend the ANA's continuing efforts to promote responsible marketing through its support of the self-regulatory programs of the Advertising Self-Regulatory Council and the Council of Better Business Bureaus. Self-regulatory programs – for national advertising, children's advertising, direct response advertising, and online behavioral advertising – can serve a critical function in policing the marketplace and are an important complement to the FTC's law enforcement work."); Jessica Rich, Director, Bureau of Consumer Protection, FTC, Remarks at NAD Annual Conference (Sept. 30, 2013) ("We have long supported BBB's self-regulatory initiatives as an important complement to the FTC's law enforcement, policy, and educational initiatives. Over the years, the FTC has emphasized that when implemented in tandem, self-regulation and government oversight provide valuable efficiencies and benefits."); Maureen Ohlhausen, Commissioner, FTC, Remarks at Digital Advertising Alliance Summit (June 5, 2013) ("I am especially pleased that DAA has not only adopted broadly applicable Principles that apply across sectors and to a wide variety of companies but also, building on the success of the advertising industry's approach to self regulation, has provided for strong, objective oversight by the Council of Better Business Bureaus (CBBB) and the Direct Marketing Association. These programs provide for prompt follow up on complaints and, in the case of the CBBB, active monitoring of all members of the digital advertising system."); Jon Leibowitz, Chairman, FTC, Remarks at White House Privacy Event (Feb. 23, 2012) ("For the past several years, the online advertising industry has been working to develop an icon that consumers could click to opt out of receiving targeted ads. Today, although it is still a work in progress, the ad industry has obtained buy-in from companies that deliver 90 percent of online behavioral advertisements; and, with the Better Business Bureau, it has established a mechanism with teeth to address non-compliance, backed up with FTC enforcement.").

enforcement, clear signs of vibrant self-regulation. The opt-in regime proposed in the NPRM is not needed and would be seriously counterproductive.

V. THE COMMISSION'S PROPOSED PRIVACY FRAMEWORK IS CONTRARY TO EXISTING, EFFECTIVE FTC PRIVACY PRINCIPLES, INCLUDING RESPECT FOR DATA CONTEXT AND SENSITIVITY

In 2012, the FTC published its seminal report on consumer privacy, *Protecting Consumer Privacy in an Era of Rapid Change* ("FTC Privacy Report").[35] The Report proposed a privacy framework built on the consensus principles that emerged from a two-year process involving multiple roundtables and over 450 comments from a diverse range of stakeholders.[36] But despite professing support for the FTC Privacy Report recommendations[37] and praising the FTC's effectiveness in protecting consumers' online privacy,[38] the NPRM ignores the primary principles of the FTC Privacy Report, including offering consumers choices based on the context of the commercial interaction and the sensitivity of the data at issue.[39] The NPRM offers little explanation or justification regarding how this significant departure from the FTC's privacy framework will benefit the public, and fails to address the confusion and opt-in decision fatigue that is likely to result from the proposed rules. Given the lack of evidence that a new framework

---

[35] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012), www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("FTC Privacy Report").

[36] *Id.* at i.

[37] NPRM ¶¶4 ("[T]his NPRM looks to learnings from the FTC and other privacy regimes to provide complementary guidance."); 18 ("[The NPRM] looks to the framework of best practices for providing consumers with privacy choices that was recommended by the FTC in its 2012 Privacy Report…"); 122 (stating that the proposed rule is consistent with "FTC best practices counsel[ing] that consumer choice turn on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business").

[38] NPRM ¶¶8 (describing the FTC's "precedent-setting consent orders addressing privacy practices on the Internet"); 132 (referencing the FTC's "robust privacy enforcement practice").

[39] FTC Privacy Report, *supra* n. 35, at vii-viii.

is necessary, the Commission should not attempt to fix what is not broken; rather, the existing privacy framework should be maintained and supported.

A. Existing Regulatory Guidance Supports Basing Rules on Data Context and Sensitivity.

One of the three pillars of the FTC's Privacy Report framework is simplified consumer choice. The foundation of this concept rests on two principles: that no consumer choice is required where data collection or use is consistent with the context of the consumer's interaction with a company, and that consumers should be offered choices appropriate to the sensitivity of the data involved.[40]

The FTC took this more flexible approach in the final version of the Privacy Report after commenters expressed concern that prescribing specific practices would stifle innovation.[41] That risk is equally, if not more, likely to be present for BIAS providers under the proposed rules. BIAS providers' collection and use of customer information that are "consistent with customer expectations" clearly include, but are by no means limited to, those proposed by the Commission.[42] As noted in the FTC Privacy Report, first-party marketing practices that do not involve uses of sensitive data "are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice."[43] By prescribing only narrow circumstances in which providers may use broad segments of customer information without opt-in approval, regardless of the data's sensitivity, the NPRM discourages BIAS providers from developing new business models and

---

[40] *Id.*

[41] *Id.* at 35-36.

[42] NPRM ¶123.

[43] FTC Privacy Report, *supra* n. 35, at 40.

connecting consumers with new products, services, and/or discounts unrelated to communications services from which they may benefit.[44]

Highly differentiated treatment of sensitive and non-sensitive data is also supported by the FTC and the National Institute for Standards and Technology ("NIST"), which are both cited by the Commission as sources for the proposed rules.[45] In its Privacy Report, the FTC defined "sensitive data" as Social Security numbers and financial, health, children's, or precise geolocation information, while classifying all other data as "non-sensitive." Likewise, the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information ("NIST PII Guide") notes that "All PII is not created equal," and suggests classifying information in accordance with "the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed."[46] Forty-seven states have followed a similar approach in adopting data breach notification laws, which require companies to notify users of a breach impacting certain types of sensitive personal information, such as Social Security numbers, driver's license numbers, usernames and passwords, and financial account information.[47]

Accordingly, any requirements regarding data collection and use should carefully take into account the sensitivity of information. In this regard, it is worth emphasizing that a vast amount of marketing data, even if potentially personally identifiable, is not sensitive data and is highly

---

[44] NPRM ¶¶112, 115 (allowing BIAS providers to use CPNI without choice for purposes necessary to the provision of network service, to market BIAS offerings in the same category of services to which the customer is already subscribed, and for enumerated statutory exceptions); ¶122 (permitting opt-out approval for marketing communications-related services).

[45] NPRM ¶60.

[46] Erika McCallister, Tim Grance & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST ES-2 (2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf ("NIST PII Guide").

[47] *See, e.g.*, Cal. Civ. Code § 1798.82(h).

unlikely to be used to harm consumers in any way. Most consumers do not consider their everyday shopping preferences, such as their proclivity for no-pulp orange juice or extra-soft tissues, to be sensitive.[48] At the same time, ANA recognizes that some consumers are especially privacy-sensitive, and therefore provides those consumers the ability to opt out of interest-based advertising. However, as FTC Commissioner Maureen Ohlhausen has noted, "too-high a privacy baseline – a biased baseline – imposes the privacy preferences of the few on the many."[49]

B. The FTC Privacy Framework Has Been Effective in Protecting Consumer Privacy, and Its Careful Differentiation of Sensitive and Non-Sensitive Data Treatment is Essential.

As the Commission itself notes, the FTC has been a leader in protecting consumer privacy by initiating enforcement actions against companies of all sizes that violate the principles enumerated in the Privacy Report.[50] While the NPRM highlights some of the FTC's major settlements with Internet giants such as Google and Facebook, it is important to note that the FTC has also routinely brought actions against companies of all sizes that have allegedly infringed on consumers' right to control uses of their personal information. Most recently, for instance, the FTC entered a consent decree with a company that purchased a popular Google Chrome extension and replaced it with a new extension that bypassed permissions on users' phones and automatically installed unwanted applications.[51]

---

[48] *See* 2016 Pew Study, *supra* n. 20, at 23 (finding that 67% of respondents would accept a free store loyalty card in exchange for sharing their shopping habits in at least some circumstances).

[49] Maureen K. Ohlhausen, Commissioner, FTC, Remarks at the George Mason University School of Law Public Policy Briefing on Privacy Regulation after Net Neutrality 6 (Mar. 20, 2016), www.ftc.gov/system/files/documents/public_statements/942823/160331gmuspeech1.pdf.

[50] NPRM ¶8.

[51] *In re Vulcan*, FTC Docket No. C-4573, FTC File No, 152-3159 (Apr. 18, 2016) (consent order).

Last year, the FTC also entered a consent decree with a retail tracking company that promised to allow consumers to opt out of in-store tracking but failed to make a mechanism for doing so available to consumers.[52] The FTC's history of robust privacy enforcement shows that the FTC Privacy Report framework provides an effective basis for holding companies accountable for violations of consumer privacy. ANA does not believe that the FCC needs to impose a new privacy regulatory framework on a system that is working effectively. Regrettably, the NPRM does not closely track the FTC Privacy Report, and, in fact, is antithetical to FTC precedent carefully developed and enforced for decades.

VI. THE PROPOSED METHOD OF SOLICITING OPT-IN APPROVAL COULD RESULT IN ONEROUS OPT-IN PROCESSES AND CUSTOMER NOTICE FATIGUE

Not only would the NPRM require customers to provide opt-in approval for most uses of their information, it would also require customers to endure a bombardment of consent choices and an onerous process for providing consent without any additional countervailing benefits.

Under the proposed rules, BIAS providers must solicit approval when they first intend to use or disclose customer information in a manner requiring approval and inform customers of the type of PI for which approval is sought, the purposes for which it will be used, and the entities to which it might be disclosed.[53] The Commission would also require customers to provide approvals via a centralized "dashboard" or other persistently available mechanism.[54] These requirements could make opting-in to interest-based digital advertising simply unworkable. To conspicuously solicit approval to use customer information for the purpose of facilitating interest-based

---

[52] *In re Nomi Technologies, Inc.,* FTC Docket No. 132-3251 (Apr. 23, 2015) (consent order).

[53] NPRM ¶140.

[54] NPRM ¶144.

advertising, BIAS providers would potentially have to use intrusive methods, such as pop-up notifications, to get customers' attention on each site they visit, many of which will be off the BIAS providers' web site.

Customers who wish to provide consent might then have to navigate back to the BIAS providers' homepage, at which point they would have to click through disclosures prior to giving consent. Such disclosures would be lengthy and complex because BIAS providers would have to disclose all potential uses of the information sought and include ancillary explanations about the extent and duration of such consent. Few, if any, customers would be willing to endure this onerous process and if these types of choices proliferate, as is likely, consumer annoyance and opt-in fatigue will increase substantially over time. Customers, in fact, may become so numb to this constant barrage of choice notifications that they may refuse to opt in altogether.

Because BIAS providers have to account for a wide variety of Internet users with varying degrees of Internet savvy, in an abundance of caution, BIAS customers will also be presented with many consent options. Data security professionals already have encountered and expressed significant concern in regard to the real dangers of data breach notice fatigue.[55] Repetitive opt-in privacy notices could similarly fatigue the customer and have the very opposite of the intended effect. Instead of becoming more privacy-aware, the consumer is more likely to tune out and become apathetic in regard to regular customer notices. That effect is evident in the EU, where websites must provide notice and seek consent before using cookies on a webpage.[56] One study,

---

[55] *See* Tracy Kitten, *Battling 'Breach Fatigue'*, Bank Info Security (May 10, 2011), www.bankinfosecurity.com/battling-breach-fatigue-a-3621; *see also* NPRM ¶236 (recognizing the harms inherent in data breach over-notification).

[56] Directive 2009/136/EC of the European Parliament and of the Council (Nov. 25, 2009), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

for example, found that 41% of site visitors do not read such "cookie notices."[57] That study also showed that such frequent notices not only failed to benefit consumers, but actually harmed them by raising website operating costs at the expense of quality content and services.[58] All told, these studies estimate that the law cost the European digital economy an estimated $1.4 billion each year, and cost the larger European economy $917 million each year in lost productivity from reading and accepting cookie notifications.[59]

Recognizing that requiring opt-in consent for cookies would have a devastating impact on the digital economy and would be detrimental to users' Internet experience, some countries such as the United Kingdom (UK) instead implemented an opt-out framework to comply with the Directive.[60] As the UK Information Commissioner's Office recognized, implementation of an opt-in framework could "significantly restrict the operation of internet services that users generally take for granted," and "would be likely to cause disproportionate inconvenience both to website providers and to users."[61] An Impact Assessment conducted by the UK's Department for Business, Innovation, and Skills predicted a similarly dire outcome, finding that if an opt-in regime was implemented, "[m]any of the most popular websites and services would be unusable or severely

---

[57] Daniel Castro & Alan McQuinn, *The Economic Costs of the European Union's Cookie Notification Policy*, The Information Technology & Innovation Foundation 7 (Nov. 2014), www2.itif.org/2014-economic-costs-eu-cookie.pdf.

[58] *Id.*

[59] *Id.* at 4-6.

[60] Charles Arthur, *Cookies law changed at 11th hour to introduce 'implied consent'*, The Guardian (May 25, 2012), www.theguardian.com/technology/2012/may/26/cookies-law-changed-implied-consent.

[61] Information Commissioner's Office, *Enforcing the revised Privacy and Electronic Communications Regulations (PECR)* (May 25, 2011), https://ico.org.uk/media/about-the-ico/policies-and-procedures/2777/enforcing_the_revised_privacy_and_electronic_communication_regulations_v1.pdf.

restricted."[62] The Commission should learn from the UK's experience and follow the guidance of FTC Commissioner Maureen K. Ohlhausen, who has warned that "opt in mandates unavoidably *reduce* consumer choice."[63]

Taken together, onerous, overly expansive privacy opt-in requirements and notice fatigue will prevent customers from being able to easily provide approvals, and will in turn effectively prevent BIAS providers and other advertisers who depend on data from these sources from participating efficiently and effectively in the digital advertising marketplace, thereby hurting the economy and consumers. The FCC should avoid implementing rules that would have these negative effects.

VII. ANY PRIVACY RULES SHOULD DIFFERENTIATE CAREFULLY BETWEEN SENSITIVE AND NON-SENSITIVE CUSTOMER INFORMATION

The Commission's proposed rules impose restrictions on BIAS providers' use of customer PI and CPNI without regard to the variation in sensitivity between different information elements included in those definitions. While all such blanket rules are inconsistent with existing regulatory frameworks, the Commission's proposal to require opt-in consent for all uses of non-sensitive customer information would have particularly drastic competitive consequences for advertising,

---

[62] Department for Business, Innovation, and Skills, *Implementing the Revised EU Electronic Communications Framework: Impact Assessment* (Sept. 2010), www.gov.uk/government/uploads/system/uploads/attachment_data/file/31568/10-1133-implementing-revised-electronic-communications-framework-impact.pdf.

[63] Maureen K. Ohlhausen, Commissioner, FTC, Remarks at Privacy Regulation in the Internet Ecosystem, Free State Foundation Eighth Annual Telecom Policy Conference 8 (Mar. 23, 2016), www.ftc.gov/system/files/documents/public_statements/941643/160323fsf1.pdf.

including BIAS providers that participate in the digital advertising ecosystem and other advertisers that would be adversely affected by the NPRM.

As demonstrated above, the opt-in requirement would also be extraordinarily burdensome for customers that wish to enjoy the benefits of digital advertising, and may confuse customers by requiring them to make multiple inconsistent privacy elections for similar types of advertisements. To avoid these potentially negative consequences, the Commission should take no action that does not carefully differentiate between sensitive and non-sensitive information, apply requirements appropriately tailored to the specific information's sensitivity, and comport with existing FTC guidance.

A. The Commission Should Not Move Forward With This NPRM. Any Action Regarding Interest-Based Advertising Must Treat "Sensitive" and "Non-Sensitive" Customer PI Consistent With Existing Regulatory Guidance and Reflect the Unique Harms Associated With Each Information Type.

As described in Section V above, the Commission's proposed rules ignore key differences in consumer expectations for sensitive and less-sensitive information. The proposal defines customer PI protected by Section 222(a) of the Communications Act of 1934 to include all "personally identifiable information" ("PII"), which in turn is defined as CPNI and "any information that is linked or linkable to an individual."[64] The examples of PII provided in the NPRM make clear that the definition encompasses both highly sensitive data, such as Social Security numbers, and non-sensitive data that most users automatically share with websites, such as IP addresses and traffic statistics.[65]

---

[64] NPRM ¶¶57, 61.

[65] *Id.* ¶62.

While ANA is concerned about "the large risks posed by unauthorized uses and disclosures" of sensitive data, such risks are undoubtedly far different for non-sensitive information.[66] Sensitive information such as Social Security numbers, payment card numbers, and detailed health information are far more likely to be stolen, misused, and/or sold for profit, resulting in considerable financial losses to consumers.[67] By contrast, the only risk cited by the Commission that could conceivably apply to non-sensitive data is the risk of reassociating anonymous data with identified individuals.[68] To the extent that this risk is not fully mitigated by contractual prohibitions on re-identifying anonymous information,[69] privacy concerns would only be implicated for the subset of users that do not want their non-sensitive information to be tracked. While the ANA takes these concerns very seriously, the unique harms associated with unauthorized disclosures of sensitive data suggest that they deserve separate consideration, consistent with existing self-regulatory standards.[70]

B. Privacy Regimes Should Support an Opt-Out Approval Framework for Uses of Non-Sensitive Customer Information.

---

[66] NPRM ¶60.

[67] *See* Kamala Harris, *California Data Breach Report* (Feb. 2016), https://oag.ca.gov/breachreport2016 (finding that "more of the most sensitive personal information – Social Security numbers and medical information – was breached than other data types").

[68] NPRM ¶60.

[69] AT&T and Verizon, for example, have committed to prohibiting their advertising partners and vendors from re-associating anonymous information or individuals for their own purposes. AT&T Privacy FAQ, www.att.com/gen/privacy-policy?pid=13692#tracking ("When we provide individual anonymous information to businesses, we require that they only use it to compile aggregate reports, and for no other purpose. We also require businesses to agree they will not attempt to identify any person using this information."); Verizon Privacy Policy, www.verizon.com/about/privacy/full-privacy-policy ("We require that these vendors and partners protect the [personal] information and use it only for the services they are providing us.").

[70] *See* Section IV, *supra.*

The Commission would require BIAS providers to seek and receive opt-in approval from their customers prior to using or sharing customer PI for purposes unrelated to marketing communications-related services.[71] This approval framework, however, is inconsistent with existing regulatory guidance and would substantially burden customers and BIAS providers alike. Consumer opt-in approval should only be required for uses and disclosures of sensitive customer information, while allowing opt-out approval for uses and disclosures of non-sensitive data.

1. An Opt-Out Framework for Non-Sensitive Customer Information Is Consistent With Existing Regulatory Guidance.

Contrary to the FCC's claim that requiring opt-in consent is "consistent with…other privacy frameworks," no other U.S. online privacy framework requires companies to obtain opt-in consent for uses of non-sensitive information.[72] As the Commission indicates in its discussion of approvals required for the use and disclosure of customer PI for marketing communications-related services,[73] the FTC Privacy Report requires companies to provide choices to consumers "for practices inconsistent with the context of their interaction with consumers."[74] The Report, however, specifies that companies need only obtain consumers' "affirmative express consent" for uses of *sensitive* data; opt-out consent is sufficient for uses of non-sensitive data.[75]

The FTC repeatedly has attempted to inform the FCC about this differentiated approach. In recent testimony before the Senate, FTC Commissioner Maureen Ohlhausen stated that, "based on the FTC's long approach in this area what we've determined is that opt-in consent is appropriate

---

[71] NPRM ¶127.

[72] *Id.*

[73] *Id.* at 127.

[74] FTC Privacy Report, *supra* n. 35 at 48.

[75] *Id.* at 58.

and a good idea for sensitive information but then, for non-sensitive information when used for things like targeted advertising, that an opt-out approach is more consistent with consumers' expectations."[76] Previously, Commissioner Ohlhausen had stated that, if "the FCC wished to be consistent with the FTC's approach of using prohibitions only for widely held consumer preferences, it would …simply require opt in for specific, sensitive uses."[77] And FTC Enforcement Bureau Director Jessica Rich reiterated this type of differentiated approach in a recent blog post.[78] While recognizing that information is "personally identifiable" when it can be reasonably linked to a particular person or device, Bureau Director Rich also wrote that "Certainly, all forms of personal information don't need the same level of protection"; rather, companies should "provide protections that are appropriate to the risks."[79]

Similarly, the NIST PII Guide provides that "[n]ot all PII should be protected in the same way. Organizations should apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level."[80]

2. An Opt-Out Framework for Non-Sensitive Customer Information Aligns With Consumer Expectations and Avoids the Confusion of Multiple Consent Frameworks.

An opt-out framework for uses of non-sensitive information also matches consumers' expectations regarding treatment of their data. Each day, consumers share many types of personal

---

[76] Maureen K. Ohlhausen, Commissioner, FTC, Remarks before the Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law, Examining the Proposed FCC Privacy Rules (May 11, 2016).

[77] Maureen K. Ohlhausen, Commissioner, FTC, Remarks at Privacy Regulation in the Internet Ecosystem, Free State Foundation Eighth Annual Telecom Policy Conference 6 (Mar. 23, 2016), www.ftc.gov/system/files/documents/public_statements/941643/160323fsf1.pdf.

[78] Jessica Rich, Director, FTC Bureau of Consumer Protection, *Keeping Up with the Online Advertising Industry* (Apr. 21, 2016), www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[79] *Id.*

[80] NIST PII Guide, *supra* n. 46, at ES-5.

information in many different ways that reflect both the sensitivity of the information at issue and the user's own privacy preferences. For instance, online banks require users to log in using a username and password (at minimum), and virtually all consumers expect that their financial information will be kept strictly confidential to guard against misuse. By contrast, users share their IP address, session IDs and browser profiles with websites by default unless they take affirmative steps to mask them. A Pew study cited by the Commission[81] also found that "certain realms are not inherently private and different rules about surveillance and sharing apply."[82] It additionally found that only 17% of consumers would never exchange their personal information for something of value.[83] Opt-out frameworks consistent with the current self-regulatory, FTC and state privacy regimes therefore match consumers' expectations while the NPRM proposal diverges dramatically from this long-standing approach.

An opt-out framework also promotes a "uniform expectation of privacy" for most online activities.[84] Advertising networks collect anonymized information about consumers' interests from a wide variety of sources, including edge providers, data brokers, and BIAS providers, for the purpose of serving interest-based advertisements.[85] Any given interest-based ad could be informed by one or more of these sources, and ads do not indicate the source of this information.

Under current regulatory and self-regulatory frameworks, consumers who wish to receive interest-based ads need not take any action, while those who do not can elect to opt-out of any

---

[81] NPRM ¶123 n.210.

[82] 2016 Pew Study, *supra* n. 20, at 6.

[83] *Id.* at 3.

[84] NPRM, Dissenting Statement of Commissioner Ajit Pai (quoting Chairman Tom Wheeler).

[85] TRUSTe, *What is Online Behavioral Advertising?*, www.truste.com/consumer-privacy/about-oba/#&panel1-1.

DAA-participating ad by clicking the "AdChoices" icon and adjusting their preferences.[86] Under the NPRM's proposed framework, however, two ads that would be indistinguishable to a consumer could be governed by two totally opposite frameworks and choice mechanisms. This result would undoubtedly cause confusion for consumers without accompanying benefits: those who wish to receive interest-based ads informed by their customer PI will likely not know that they need to opt in via their provider's website, and those that do not may be confused by having to opt out of some ads but not others. The proposed rule would also disadvantage BIAS providers that operate demand-side advertising platforms, as they would not be able to use their own information to deliver ads.

Opt-in approval should only be required for sensitive customer information, while opt-out approval should be allowed for uses of non-sensitive customer information.

VIII. PROPOSED DATA BREACH NOTIFICATION REQUIREMENTS WILL ENCOURAGE THE PREMATURE RELEASE OF INACCURATE INFORMATION

In the NPRM, the Commission proposes more extensive data breach notification requirements than existing data breach requirements for voice service.[87] ANA believes that changes in data security law and regulation should be left to the Congress, but it is especially concerned that the proposed timetable for this notice is unreasonable and likely to be detrimental.

Upon discovery of a "breach," the NPRM would require carriers and BIAS providers to:

[86] Digital Advertising Alliance, *YourAdChoices Gives You Control*, http://youradchoices.com/control.

[87] NPRM ¶¶ 233-255.

- Notify affected customers of breaches of customer PI no later than 10 days after the discovery of the breach, subject to law enforcement needs, under circumstances enumerated by the Commission;
- Notify the Commission of any breach of customer PI no later than 7 days after discovery of the breach; and
- Notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service of breaches of customer PI reasonably believed to relate to more than 5,000 customers no later than 7 days after discovery of the breach, and at least 3 days before notification to customers.

Among other issues, the NPRM's inflexible timetable often would force BIAS providers to provide notice before the nature and extent of the incident has been ascertained, which might undermine law enforcement efforts. During a data breach, it frequently takes several days, and sometimes weeks, to understand the true facts surrounding an incident. ANA notes that any time period less than a 30-day time frame is clearly unreasonable, though in complicated breach scenarios, even that time period might be insufficient. A longer time period would provide companies some leeway to retain outside forensics consultants, where necessary, in order to fully evaluate the facts of any suspected incident. Additionally, if requested by law enforcement, any breach notification should be allowed to be extended for a longer period to help resolve issues of criminality that might be involved.

The Commission requested further comments on whether to limit breach notification in certain circumstances, and what should be the appropriate trigger (*e.g.*, likelihood of misuse of the data or the number of affected consumers). Breach notification should be limited only to areas where there is a strong likelihood of harm to the public. To require notification where harm is at best highly speculative would not benefit consumers and might, as noted, create notice fatigue.

Where a BIAS provider can ensure that customer data will not be misused and no harm has occurred to the customer, there should not be a need for breach notice.

If a BIAS provider, for example, receives an affidavit of data destruction from an individual inadvertently receiving data whereby the provider has reasonable assurances that the data will not be used for identity theft or, if no data released could likely result in BIAS account access or other account access, the provider's breach alert will simply become yet another repetitive piece of annoying and non-productive consumer notification. This type of useless notification is highly likely for large segments of non-sensitive marketing data where access to the information, even if personally identifiable, is highly unlikely to be used to harm anyone. To avoid perpetuating data breach notice fatigue, consumers should only be notified when it is necessary for them to take action.

IX. THE COMMISSION'S PROPOSED RULES VIOLATE THE FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION

Like the rules invalidated by the Tenth Circuit in *U.S. West Inc. v FCC*, 182 F.3d 1224 (10th Cir. 1999), the Commission's proposed broadband privacy rules unconstitutionally restrict commercial speech in violation of the First Amendment.

As a threshold matter, there can be no question that the proposed rules would restrict speech.[88] Under the proposed rules, BIAS providers would be prohibited from using information in their possession to market non-communications-related services without customers' opt-in consent.[89] This constitutes a "restriction on speech tailored to a particular audience," or "targeted

[88] *U.S. West Inc. v FCC*, 182 F.3d 1224 at 1232 ("As a threshold requirement for the application of the First Amendment, the government action must abridge or restrict protected speech.").

[89] NPRM ¶127.

speech."[90] It is of no consequence that BIAS providers could indiscriminately send advertisements to individuals without using their customers' PI, as "the existence of alternative channels of communication" does not negate the existence of a burden on targeted speech.[91]

As the speech at issue "propose[s] a commercial transaction," it constitutes commercial speech.[92] As the Supreme Court has long made clear, "[t]he commercial market place, like other spheres of our social and cultural life, provides a forum where ideas and information flourish. Some of the ideas and information are vital, some of slight worth. But the general rule is that the speaker and the audience, not the government, assess the value of the information presented. Thus, even a communication that does no more than propose a commercial transaction is entitled to the coverage of the First Amendment."[93] Regulations of lawful, non-misleading commercial speech are valid only if they satisfy the factors set forth by the United States Supreme Court in *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York:*[94] (1) there is a "substantial state interest in regulating the speech"; (2) "the regulation directly and materially

---

[90] *U.S. West*, 182 F.3d at 1232; *see also Verizon Nw., Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1190 (W.D. Wash. 2003) (explaining in a case involving Washington State restrictions on CPNI usage that "the rules do, however, indirectly affect Verizon's marketing by requiring prior customer approval for the use of CPNI in both developing and targeting that marketing," which therefore implicates speech).

[91] *U.S. West*, 182 F.3d at 1232.

[92] *Id. See also Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011) (explaining that information regarding doctors' prescribing methods is commercial speech because "the creation and dissemination of information are speech within the meaning of the First Amendment. . . . Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes").

[93] *Edenfield v. Fane*, 113 S. Ct. 1792, 1798 (1993).

[94] *C. Hudson Gas & Elec. Corp. v. Pub. Serv. Commn. of New York*, 447 U.S. 557 (1980).

advances that interest"; and (3) "the regulation is no more extensive than necessary to serve the interest."[95] The Commission's proposed regulations fail all three prongs of this test.

Although the Commission proposes to prohibit BIAS providers from using customer PI to market anything except communications-related services because such uses would purportedly violate customers' privacy expectations,[96] as the Tenth Circuit made clear in *U.S. West*, "[i]n the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity."[97] The Commission offers no explanation as to why allowing BIAS providers to use customer PI to market non-communications-related services would result in any of these consequences.

While the Commission theorizes that "increasing the number of entities that have access to customer PI logically increases the risk of unauthorized disclosure," it does not cite any evidence that disclosures of undifferentiated categories of customer PI have resulted in identity theft, that BIAS providers are more susceptible to such risks than any other entity, or that disclosures would result in embarrassment, intimidation, or harassment.[98] Without such evidence, the Commission cannot claim that it has a substantial interest in prohibiting BIAS providers from using or

---

[95] *U.S. West*, 162 F.3d at 1233 (quoting *Revo v. Disciplinary Bd. of the Supreme Court for the State of N.M.*, 106 F.3d 929, 932 (10th Cir. 1997)); *see also Turner Broadcasting Inc. v. FCC*, 512 U.S., 622 at 662–663, 114 S.Ct. 2445 (explaining that these standards ensure not only that the State's interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message).

[96] *See* NPRM ¶109.

[97] *U.S. West*, 182 F.3d at 1235.

[98] NPRM ¶129.

disclosing customer PI for marketing non-communications-related services, or that the regulations materially advance such an interest. Moreover, as explained in this filing, interest-based advertising does not in fact run counter to consumers' privacy expectations; instead, such speech has become a welcome, expected, and useful form of advertising for consumers that plays an important role in providing them ever-increasing amounts of free Internet content.

Furthermore, consumers who do not want interest-based advertising can opt out of receiving it; therefore, even if the Commission could demonstrate that the proposed regulations advance a substantial interest, the proposal is far more extensive than necessary to serve any such interest.[99] First, as explained above, the proposed regulations prohibit BIAS providers' use and disclosure of *all* customer PI without an opt-in, not just sensitive customer information. Despite the Commission's claims that these sweeping rules are necessary because customer PI is "interrelated" and that there are "large risks posed by unauthorized uses and disclosures," it offers no evidence that intentional uses or disclosures of non-sensitive information have ever caused consumers any tangible harm.[100] Second, the NPRM does not demonstrate that the FCC "adequately consider[ed] an obvious and substantially less restrictive alternative, an opt-out strategy," which is consistent with the approach taken for interest-based advertising in most other industries.[101] The proposed regulations therefore are not narrowly tailored.

---

[99] *U.S. West*, 182 F.3d at 1238 (quoting *Rubin v. Coors Brewing Co.*, 514 U.S. 476 at 486) (explaining that to satisfy the "narrow tailoring" prong of the Central Hudson test, the government must demonstrate that the regulations are "no more extensive than necessary to serve the stated interests"); *see also Bd. of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989).

[100] NPRM ¶60.

[101] *U.S. West*, 182 F.3d at 139; see also *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993) ("To be narrowly tailored, the government's speech restriction must signify a careful calculation of the costs and benefits associated with the burden on speech imposed by its prohibition."); *Verizon Nw., Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1195 (W.D. Wash. 2003) (holding that Washington State did not have a legitimate interest in imposing an opt-in regime on certain providers regarding CPNI usage when an opt-out approach would impose a far lesser burden on speech).

The NPRM's encroachment on BIAS providers' First Amendment rights will also have downstream effects on the speech interests of other advertisers. Inappropriately burdening BIAS providers' collection and use of data will result in that data often not being available to other advertisers trying to convey information to consumers, thereby denying consumers access to that valuable information for purchasing and other decisions. ANA has just begun to assess the First Amendment implications of all these limitations on the entire advertising and marketing ecosystem, but it is clear that the NPRM will impose constraints that are unnecessary, limit speech, and are overly burdensome. The proposed regulations unconstitutionally burden BIAS providers' and other advertisers' rights to commercial speech in violation of the First Amendment.

X. INTERESTED STAKEHOLDERS HAVE NOT BEEN PROVIDED SUFFICIENT TIME TO COMMENT ON THIS MATTER IN VIOLATION OF TITLE 5, UNITED STATES CODE

ANA reiterates the concerns it raised in its April 11, 2016 letter to the Commission objecting to the fifty-seven day window for comments on the NPRM.[102] With more than 500 detailed questions, the ability to provide thoughtful answers on a wide range of critical issues was highly constrained by the overly tight deadlines. Given the exceptional length and complexity of the NPRM, section 553(b) and (c) of title 5, United States Code, requires that the Commission provide additional time for interested stakeholders to comment on this proceeding.

Courts have held that Section 553 "requires an agency to publish 'notice' of 'either the terms or substance of the proposed rule or a description of the subjects and issues involved,' in order to 'give interested persons an opportunity to participate in the rulemaking through

[102] Request for Extension of Time, Assoc. of Nat'l Advertisers, Dkt. No. 16-106 (Apr. 11, 2016).

submission of written data, views, or arguments.'"[103] In considering whether an agency has complied with this requirement, courts "inquire whether the notice given affords 'exposure to diverse public comment,' 'fairness to affected parties,' and 'an opportunity to develop evidence in the record.'"[104] Here, the Commission's provision of a fifty-seven day notice period before the comment deadline does not meet these legal standards and significantly hinders the public's ability to comment on the multitude of complex questions posed in the extremely lengthy NPRM.

The nuanced questions posed within this NPRM (and specifically those requesting information regarding the impact to the advertising industry at paragraph 132) require data and economic study. The present timetable gave the ANA, and many of its more than 700 members, insufficient opportunity to derive data on many important and weighty questions concerning consumer privacy and ad ecosystem impacts. These include, among others:

- Potential cost increases for broadband service;
- Impact on ad networks' revenue;
- Potential costs of compliance; and
- Appropriate standards for de-identifying information, and many others.

It is insufficient to assert, as the Commission did in denying requests for an extension of time to comment on the NPRM, that the short timeframe was warranted because the FCC does not believe that "the scope of the Broadband Privacy NPRM was unanticipated."[105] It is one thing to indicate that it is the intent to take some action, and a far different thing to actually set forth

[103] *Pharm. Research & Manufacturers of Am. v. Fed. Trade Comm'n*, 44 F. Supp. 3d 95, 136 (D.D.C. 2014) (quoting *Am. Radio Relay League, Inc. v. FCC*, 524 F.3d 227, 236 (D.C. Cir. 2008)).

[104] *Nat'l Min. Ass'n v. Mine Safety & Health Admin*., 116 F.3d 520, 531 (D.C. Cir. 1997) (quoting *Association of Am. Railroads v. Dep't of Transp*., 38 F.3d 582, 589 (D.C. Cir. 1994)).

[105] *In the Matter of Protecting the Privacy of Customer of Broadband and Other Telecommunications Services*, Order of the Wireline Competition Bureau, WC Dkt No. 16-106 at 3 (Apr. 29, 2016).

extensive and very specific proposals that require (and request) review and comment. The FCC has deprived many interested parties of a sufficient opportunity to comment on this rulemaking and to submit evidence for the record in violation of Section 553. The ANA and its members cannot collect accurate, complete data on these technical and complex questions as requested by the NPRM in the short timeframe provided.

XI. CONCLUSION

For the foregoing reasons, ANA urges the Commission to refrain from approving the NPRM in its current form. The rules are unnecessary in light of effective existing law and self-regulatory standards. Further, the proposed expanded opt-in consent rules would jeopardize the significant contributions made by advertising to the economic and other interests of the public. These proposals completely fail to adequately differentiate the various levels of sensitivity of data, when existing privacy self-regulatory standards and state and FTC enforcement efforts take great care to do so. The Commission must engage in a thoughtful, deliberate and thorough evaluation of the potential impacts of the proposed rules, something that the limited time provided for the initial comment period does not permit either for the Commission or interested parties.

These rules should not be adopted because they clearly do not promote the public interest.

Respectfully Submitted,

Dan Jaffe
Group Executive Vice President, Government Relations
Association of National Advertisers (ANA)
2020 K Street, NW - Suite 660
Washington, D.C. 20006
Phone: 202.296.1883
Fax: 202.296.1430